

Message

From: Jose Arteaga [j.arteaga@netzero.net]
Sent: 10/1/2020 10:57:43 AM
To: Alex Azar [alex.azar@hhs.gov]; Wheeler, Andrew [wheeler.andrew@epa.gov]; Ben Carson [ben.carson@hud.gov]; Chad Wolf [dhsexecsec@hq.dhs.gov]; Dan Brouillette [dan.brouillette@energy.gov]; David Bernhardt [david.berhardt@ios.doi.gov]; Elaine Chao [elaine.chao@dot.gov]; Elisabeth "Betsy" Prince DeVos [betsy.devos@ed.gov]; Eugene Scalia [executivesecretariat@dol.gov]; Federal Whistleblower ['DHSOIGHOTLINE@dhs.gov']; Gina Haspel [john.edwards@cia.gov]; John Ratcliffe [john.ratcliffe@dni.gov]; Jovita Carranza [jovita.carranza@sba.gov]; Kelly Craft [kelly.craft@un.org]; Mark Esper [mark.esper@dod.gov]; Mark Meadows [mark.meadows@whitehouse.gov]; Megan Smith [Ex. 6 Personal Privacy]; Mike Pence [info@mike.pence.com]; Mike Pompeo [mike.pompeo@state.gov]; President Donald Trump [info@donaldtrump.com]; Robert E. Lighthizer [Ex. 6 Personal Privacy]; Robert Wilkie [robert.wilkie@va.gov]; Russ Vought [Ex. 6 Personal Privacy]; Sonny Perdue [sonny.perdue@usda.gov]; Steve Mnuchin [steve.mnuchin@treasury.gov]; Wilbur Ross [wilbur.ross@commerce.gov]; William Barr [william.barr@justice.gov]
Subject: FW: Securing your website (Updated 7/24/2020) (1 of 14)

From: Jose Arteaga [mailto:j.arteaga@netzero.net]
Sent: Thursday, October 01, 2020 3:57 AM
To: Christopher Rein (opsonduty@mmuair.com); Michael Schubach (michael.schubach@trump.com); Michael Schubach (donald.trump@trump.com); Michael Schubach (allen.weisselberg@trump.com); 'Diana.Gonzalez@oshe.nj.gov'; 'Nicole.Kirgan@oshe.nj.gov'; 'Stefani.Thachik@oshe.nj.gov'; 'publicinfo@co.somerset.nj.us'; 'ITDiv@co.somerset.nj.us'; 'PublicInfo@co.somerset.nj.us'; 'FreeholdersOffice@co.somerset.nj.us'
Cc: Christopher Rein (christopher.rein@state.nj.us); Christopher Rein (governor@state.nj.us); Christopher Rein (feedback@sos.nj.gov)
Subject: Securing your website (Updated 7/24/2020) (1 of 14)

Póngase en contacto con Servicio Commercial de EE.UU. <https://2016.export.gov/usoffices/index.asp> o *Web Network Shield* (WNS) 480-318-8020 o 418-271-6176 para una traducción en su idioma de elección.

01010111 01000101 01000010 00100000 01001110 01000101 01010100 01010111 01001111 01010010
01001011 00100000 01010011 01001000 01001001 01000101 01001100 01000100®

WNS®

Secure by Design

“Action without information is dangerous. Information without action is futile.” ~ Arizona Tax Research Association

President Trump's schedule for October 1, 2020

1:55 PM The President arrives at Morristown Municipal Airport

2:20 PM The President arrives at Bedminster Landing Zone Trump National Golf Club, Bedminster

3:00 PM The President participates in a roundtable with supporters

3:45 PM The President delivers remarks at a fundraising committee reception

4:55 PM The President has left Bedminster, NJ

Data breaches continue to plague government organizations¹

Data breaches continue to plague education institutions²

Data breaches continue to plague distance learning

(August 22, 2020) <http://www.bing.com/search?q=distance+learning+data+breach+hack+attack&src=IE-SearchBox&FORM=IENTTR&conversationid=>

Cyber-crime in the U.S. has been declared a national emergency eight (8) times. Since 2017, lack of cyber-security has cost tax payers \$27 billion to \$56 billion per day. The average cost of a data breach has increased \$106.5M (>1100%) from 2017 to 2020.³

90% of small businesses that have customer information stolen go out of business within three years.⁴

This simply shouldn't be happening six years after we introduced WNS, our proven effect cyber-security product against all forms of URA. We strongly urge the federal government to pay the revenue owed to Jose Arteaga in the form of a legal out-of-court settlement for violation of Jose Arteaga's civil rights for thirty-nine (39) years and violation of Web Network Shield's Sherman Act rights for six (6) years. Then we can begin the process of securing the entire country from all forms of URA ASAP.

WNS (Web Network Shield) has successfully demonstrated the effectiveness of its cyber-security product WNS to prevent all forms of URA (unauthorized remote access) to the New York Times, Wall Street Journal, Walmart, AT&T, Arizona Department of Water Resources, the U.S. Department of Defense, the U.S. House of Representatives, the U.S. Senate, The White House, the cities of Dallas, Phoenix, Tucson, Yuma, San Diego, Los Angeles, San Francisco, Sacramento, Washington D.C., New York City, Reno, the Trump Organization, the Catholic Church, the United Nations, Ohio and San Diego State University.

On September 12, 2020, while preparing a presentation for the city of Reno, NV, I needed to visit the city of Reno's website <https://www.reno.gov/>. Unfortunately, there was a phishing malware program located within the city of Reno's website. Fortunately, WNS was able to prevent URA (unauthorized remote access) as a result of that malware program.

"Show, don't tell" ~ Storytellers

WNS wants to help protect your children, workers, and businesses from all forms of URA (unauthorized remote access). WNS will provide your organizations a free sample of part of our secure WNS web browser. If successful, the free demonstration will secure your websites only, not your IoT devices, from all forms of URA (unauthorized remote access).

Currently, WNS (Web Network Shield) has added your websites <https://www.co.somerset.nj.us/>,
<https://www.mmuair.com/>, <https://www.trumpnationalbedminster.com/>,

<https://www.nj.gov/education/>, and
https://www.nj.gov/highereducation/colleges/schools_sector.shtml to our favorite websites
list. This may improve the cyber-security of your websites.

Today, October 1, 2020, at approximately 2:30 PM (EDT), WNS will remove
<https://www.co.somerset.nj.us/>, <https://www.mmuair.com/>,
<https://www.trumpnationalbedminster.com/>, <https://www.nj.gov/education/>, and
https://www.nj.gov/highereducation/colleges/schools_sector.shtml from our favorite websites
list. This may affect the cyber-security of your websites.

“An ounce of prevention is worth a pound of cure response” ~ Benjamin Franklin (sort of)

WNS provides the following protection benefits:

- There is no need to obfuscate your email address because WNS protects your email address from phishing scams by immediately detecting and preventing all forms of URA (unauthorized remote access);
- There is no need to repeatedly change your username, password, or email address because WNS protects your email address by immediately detecting and preventing all forms of URA;
- WNS eliminates the need to update your security software (i.e. download malware and spyware URLs on your hard drive) because WNS debugs all all forms of URA. Downloading more than 350,000 malware strains daily will “crash” your device’s hard drive and render your device unusable;
- Protects your information against all forms of URA even if the attacker has your user name, password, and IP address.
- Provides a browser speed not throttled by spyware and/or extensions used to track user activity;
- Pass a penetration test from all forms of URA;
- Immediately detect and prevent all forms of URA;
- Secure a data transmission up to 200 feet.

“The cyber-attacks will continue until cyber-security improves” ~ a Hacker

It has been said it will require at least 12-18 months for an effective COVID-19 vaccine to be developed and distributed. The same can be said for the secure WNS web browser.

If President Trump doesn’t immediately begin the process of preparation, production and distribution of the secure WNS web browser, the U.S. may not be cyber-secure until 2022.

If you believe cyber securing your website by preventing all forms of URA (unauthorized remote access) is important, contact your Representative to prevent all forms of URA ASAP.

The WNS web browser is free to download.⁵ Contact your Representative
<https://www.house.gov/representatives/find-your-representative>, Senator

https://www.senate.gov/general/contact_information/senators_cfm.cfm, U. S. Commercial Service <https://2016.export.gov/usoffices/index.asp> or Web Network Shield 480-318-8020 to protect your devices and information.

Web Network Shield mission statement:

Web Network Shield (WNS) seeks to become customer-focused, focusing our strategies and budgets on the technologies, systems and processes that win, serve and retain customers by immediately detecting and preventing URA from unregistered URLs, brute force programs, and mimicked IP addresses.

¹ The U.S. Outsources Cybersecurity & Defense To Contractors That Keep Getting Hacked

(May 3, 2013) <https://thinkprogress.org/the-u-s-outsources-cybersecurity-defense-to-contractors-that-keep-getting-hacked-abcb8b5a0c0a/>

Since 2005 over 9,000 data breaches have affected over 11.58 million records

(March 27, 2019) <https://www.privacyrights.org/data-breaches>

At least 693 breaches of government organizations have affected over 33.3 million records

(May 9, 2018)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=federal&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=federal&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=federal&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=state&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=state&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=state&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=county&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=county&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=county&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=city&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=city&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=city&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[11 tid%5B%5D=276&taxonomy vocabulary 11 tid%5B%5D=275&taxonomy vocabulary 11 tid%5B%5D=274&taxonomy vocabulary 11 tid%5B%5D=273&taxonomy vocabulary 11 tid%5B%5D=272&taxonomy vocabulary 11 tid%5B%5D=271&=Search+Data+Breach](#)

² Education sector not taking \$7,370,000/year cyber threat cost seriously

(September 18, 2019) <https://pressreleases.responsesource.com/news/98403/education-sector-not-taking-7-370-000-year-cyber-threat-cost-seriously/>

Universities fail to learn the importance of cybersecurity, suffering over five devastating cyber attacks a semester.

... the education sector is one of the most heavily targeted industries by cyberattacks in its 2019 Global DNS Threat Report.

Over 500 US schools were hit by ransomware in 2019

Fifteen US school districts, accounting for 100 schools, were hit in the past two weeks alone.

(October 1, 2019) <https://www.zdnet.com/article/over-500-us-schools-were-hit-by-ransomware-in-2019/>

... found and tracked ransomware infections at 54 educational organizations like school districts and colleges, accounting for disruptions at over 500 schools.

To make matters worse, the attacks seem to have picked up in the last two weeks, with 15 school districts (accounting for over 100 K-12 schools) getting hit at the worst time possible -- in the first weeks of the new school year.

Overall, Connecticut saw ransomware infections hit seven school districts throughout 2019, making them the state whose educational institutions were compromised the most by ransomware attacks this year.

... based on currently available information we know that Crowder College of Neosho, Missouri, reported receiving the highest ransom demand among all school districts, with hackers requesting a whopping \$1.6 million to provide the district with means to decrypt its systems.

Last week, the US Senate passed a bill named the DHS Cyber Hunt and Incident Response Teams Act, which would create incident response teams to help private and public entities defend against cyber-attacks, such as ransomware attacks. The bill previously passed the House floor and is expected to be signed into law by the President in the coming months.

Over 1160 breaches of education organizations have affected over 43.6 million records¹

(May 10, 2018)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=school&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy vocabulary 11 tid%5B%5D=2434&taxonomy vocabulary 11 tid%5B%5D=2257&taxonomy vocabulary 11 tid%5B%5D=2122&taxonomy vocabulary 11 tid%5B%5D=1473&taxonomy vocabulary 11 tid%5B%5D=1153&taxonomy vocabulary 11 tid%5B%5D=513&taxonomy vocabulary 11 tid%5B%5D=306&taxonomy vocabulary 11 tid%5B%5D=276&taxonomy vocabulary 11 tid%5B%5D=275&taxonomy vocabulary 11 tid%5B%5D=274&taxonomy vocabulary 11 tid%5B%5D=273&taxonomy vocabulary 11 tid%5B%5D=272&taxonomy vocabulary 11 tid%5B%5D=271&=Search+Data+Breach)

[breaches?title=school&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy vocabulary 11 tid%5B%5D=2434&taxonomy vocabulary 11 tid%5B%5D=2257&taxonomy vocabulary 11 tid%5B%5D=2122&taxonomy vocabulary 11 tid%5B%5D=1473&taxonomy vocabulary 11 tid%5B%5D=1153&taxonomy vocabulary 11 tid%5B%5D=513&taxonomy vocabulary 11 tid%5B%5D=306&taxonomy vocabulary 11 tid%5B%5D=276&taxonomy vocabulary 11 tid%5B%5D=275&taxonomy vocabulary 11 tid%5B%5D=274&taxonomy vocabulary 11 tid%5B%5D=273&taxonomy vocabulary 11 tid%5B%5D=272&taxonomy vocabulary 11 tid%5B%5D=271&=Search+Data+Breach](#)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=education&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy vocabulary 11 tid%5B%5D=2434&taxonomy vocabulary 11 tid%5B%5D=2257&taxonomy vocabulary 11 tid%5B%5D=2122&taxonomy vocabulary 11 tid%5B%5D=1473&taxonomy vocabulary 11 tid%5B%5D=1153&taxonomy vocabulary 11 tid%5B%5D=513&taxonomy vocabulary 11 tid%5B%5D=306&taxonomy vocabulary 11 tid%5B%5D=276&taxonomy vocabulary 11 tid%5B%5D=275&taxonomy vocabulary 11 tid%5B%5D=274&taxonomy vocabulary 11 tid%5B%5D=273&taxonomy vocabulary 11 tid%5B%5D=272&taxonomy vocabulary 11 tid%5B%5D=271&=Search+Data+Breach)

[breaches?title=education&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy vocabulary 11 tid%5B%5D=2434&taxonomy vocabulary 11 tid%5B%5D=2257&taxonomy vocabulary 11 tid%5B%5D=2122&taxonomy vocabulary 11 tid%5B%5D=1473&taxonomy vocabulary 11 tid%5B%5D=1153&taxonomy vocabulary 11 tid%5B%5D=513&taxonomy vocabulary 11 tid%5B%5D=306&taxonomy vocabulary 11 tid%5B%5D=276&taxonomy vocabulary 11 tid%5B%5D=275&taxonomy vocabulary 11 tid%5B%5D=274&taxonomy vocabulary 11 tid%5B%5D=273&taxonomy vocabulary 11 tid%5B%5D=272&taxonomy vocabulary 11 tid%5B%5D=271&=Search+Data+Breach](#)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=university&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy vocabulary 11 tid%5B%5D=2434&taxonomy vocabulary 11 tid%5B%5D=2257&taxonomy vocabulary 11 tid%5B%5D=2122&taxonomy vocabulary 11 tid%5B%5D=1473&taxonomy vocabulary 11 tid%5B%5D=1153&taxonomy vocabulary 11 tid%5B%5D=513&taxonomy vocabulary 11 tid%5B%5D=306&taxonomy vocabulary 11 tid%5B%5D=276&taxonomy vocabulary 11 tid%5B%5D=275&taxonomy vocabulary 11 tid%5B%5D=274&taxonomy vocabulary 11 tid%5B%5D=273&taxonomy vocabulary 11 tid%5B%5D=272&taxonomy vocabulary 11 tid%5B%5D=271&=Search+Data+Breach)

[breaches?title=university&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy vocabulary 11 tid%5B%5D=2434&taxonomy vocabulary 11 tid%5B%5D=2257&taxonomy vocabulary 11 tid%5B%5D=2122&taxonomy vocabulary 11 tid%5B%5D=1473&taxonomy vocabulary 11 tid%5B%5D=1153&taxonomy vocabulary 11 tid%5B%5D=513&taxonomy vocabulary 11 tid%5B%5D=306&taxonomy vocabulary 11 tid%5B%5D=276&taxonomy vocabulary 11 tid%5B%5D=275&taxonomy vocabulary 11 tid%5B%5D=274&taxonomy vocabulary 11 tid%5B%5D=273&taxonomy vocabulary 11 tid%5B%5D=272&taxonomy vocabulary 11 tid%5B%5D=271&=Search+Data+Breach](#)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=college&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy vocabulary 11 tid%5B%5D=2434&taxonomy vocabulary 11 tid%5B%5D=2257&taxonomy vocabulary 11 tid%5B%5D=2122&taxonomy vocabulary 11 tid%5B%5D=1473&taxonomy vocabulary 11 tid%5B%5D=1153&taxonomy vocabulary 11 tid%5B%5D=513&taxonomy vocabulary 11 tid%5B%5D=306&taxonomy vocabulary 11 tid%5B%5D=276&taxonomy vocabulary 11 tid%5B%5D=275&taxonomy vocabulary 11 tid%5B%5D=274&taxonomy vocabulary 11 tid%5B%5D=273&taxonomy vocabulary 11 tid%5B%5D=272&taxonomy vocabulary 11 tid%5B%5D=271&=Search+Data+Breach)

[breaches?title=college&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy vocabulary 11 tid%5B%5D=2434&taxonomy vocabulary 11 tid%5B%5D=2257&taxonomy vocabulary 11 tid%5B%5D=2122&taxonomy vocabulary 11 tid%5B%5D=1473&taxonomy vocabulary 11 tid%5B%5D=1153&taxonomy vocabulary 11 tid%5B%5D=513&taxonomy vocabulary 11 tid%5B%5D=306&taxonomy vocabulary 11 tid%5B%5D=276&taxonomy vocabulary 11 tid%5B%5D=275&taxonomy vocabulary 11 tid%5B%5D=274&taxonomy vocabulary 11 tid%5B%5D=273&taxonomy vocabulary 11 tid%5B%5D=272&taxonomy vocabulary 11 tid%5B%5D=271&=Search+Data+Breach](#)

[%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](#)

BACK TO SCHOOL

(December 13, 2018) <https://www.politico.com/newsletters/morning-cybersecurity>

The education sector comes in dead last when it comes to cybersecurity in 17 U.S. industries examined...

Identity theft isn't just an adult problem. Kids are victims, too

(April 28, 2018) <https://www.cnn.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html>

Child ID theft risks

Minors face some of the same risks as adults do, with their information being compromised in data breaches.

While adults make prime targets for their account balances, the "blank slate" a child provides can enable a criminal to do more damage by opening new lines of credit before someone catches on.

Protecting your kids

... experts say untangling identity theft and fraud committed against a minor is just as complicated as when an adult is the victim.

³ Cybercrime has cost more than \$10 trillion...

(October 27, 2017) <http://www.winknews.com/2017/10/27/cybercrime-has-cost-more-than-10-trillion-how-you-can-protect-yourself/>

Over \$27 billion per day!

Cost of cybercrime likely to hit \$21 trillion by 2021

(October 15, 2019) <https://www.ghanaweb.com/GhanaHomePage/business/Cost-of-cybercrime-likely-to-hit-21-trillion-by-2021-Ursula-789080>

Over \$56 billion per day!

Top 10 Most Expensive Disasters in U.S. History

(December 13, 2013) <https://www.trustedchoice.com/insurance-articles/weather-nature/most-expensive-disasters/>

1. Hurricane Katrina

•Cost: \$149 Billion

•Fatalities: 1,836

Why Cybersecurity Should Be A No. 1 Business Priority For 2017

(March 20, 2017) <https://www.forbes.com/sites/eycybersecurity/2017/03/20/why-cybersecurity-should-be-a-no-1-business-priority-for-2017/#371701681719>

Despite the evidence, most companies greatly understate the risk of a cyber incident...

This complacency makes little sense given the sharp uptick in hacking methods and sophistication. The average annual cost of cyberattacks to companies worldwide is pegged at more than \$9.5 million...

Report: Average data breach costs public companies \$116m

(June 9, 2020) <https://www.complianceweek.com/cyber-security/report-average-data-breach-costs-public-companies-116m/29037.article>

... the average cost of a cyber-breach to a publicly traded company was \$116 million.

... the most common methods hackers successfully used to obtain company data from 2011 to 2019 was malware (34 percent)...

"One of the clear problems that we identified in the work of the commission was the fact that cyber responsibilities and accountability is scattered all over the federal government and there is no oversight and no consistent accountability..."

⁴ Why the 1# Vulnerability for Cyber Attacks Will Be Apathy

(March 17, 2015) http://www.circleid.com/posts/20150317_why_the_1_vulnerability_for_cyber_attacks_will_be_apathy/

How much do hackers love small companies? Some statistics:

- The U.S. Department of Homeland Security reports that 31 percent of all cyberattacks on business were aimed at companies with fewer than 250 employees.
- Symnatec Security Response discovered in 2012 that more than half of all targeted attacks focused on those businesses with fewer than 2,500 employees.
- Verizon's 2013 Data Breach Investigations Report said that mid-sized and small businesses experienced more data breaches than did larger firms.

Perhaps most frightening is the National Cyber Security Alliance's finding in 2012 that about 60 percent of all small companies go out of business within six months of a data breach!

Average American had personal data stolen at least 4 times last year, report says

(May 15, 2020) <https://www.foxnews.com/tech/average-american-personal-data-stolen-rates>

We have some catching up to do on cyber-security

(February 20, 2015) <http://www.marketplace.org/topics/tech/big-book/we-have-some-catching-do-cyber-security>

Interviewed By Kai Ryssdal, Produced by Tommy Andres

- The Poneman Institute estimates it costs a company \$188 for every customer record stolen, from stopping the leak, bringing in outside consultants, replacing credit cards, lawsuits, etc. About 90 percent of small businesses that have customer information stolen go out of business within three years of an attack.

Cybersecurity: A Problem Too Big for Small Business to Ignore

As hackers turn increasingly to smaller, softer targets, even sole proprietors need to focus hard on cyber-risk.

(September 1, 2020) <https://www.theatlantic.com/sponsored/atl/cybersecurity-big-problem-for-small-business/1148/>

Above all, she says, "don't make it easy for cyber criminals."

Web Network Shield agrees. The articles above are particularly relevant to the state of Arizona since the majority of Arizona businesses qualify as small businesses with fewer than 1,000 customers. In the state of Arizona, data breach notification laws apply only to data breaches affecting more than 1,000 individuals.

⁵ Lifeline Program for Low-Income Consumers

(April 27, 2020) <https://www.fcc.gov/general/lifeline-program-low-income-consumers>

Since 1985, the Lifeline program has provided a discount on phone service for qualifying low-income consumers to ensure that all Americans have the opportunities and security that phone service brings, including being able to connect to jobs, family and emergency services. Lifeline is part of the Universal Service Fund. The Lifeline program is available to eligible low-income consumers in every state, territory, commonwealth, and on Tribal lands.

The Federal government will subsidize the cost of WNS in a program similar to subsidized cell phones, HUD Section 8 rent, and medical insurance.

This electronic message, including any attachments, is for the use of the intended recipient(s) only. If you have received this message in error, please notify the sender immediately and then delete it. Measures have been taken to eliminate the risk of transmitting software viruses but please be advised to conduct your own virus checks on any attachment to this message. If you are the intended recipient and you do not wish to receive similar electronic messages from us in the future then please respond to the sender to this effect.

01010100 01101000 01100101 00100000 01101111 01101110 01101100 01111001 00100000 01110100
01101000 01101001 01101110 01100111 00100000 01111001 01101111 01110101 00100000 01110111
01101001 01101100 01101100 00100000 01110010 01100101 01100111 01110010 01100101 01110100
00100000 01101001 01110011 00100000 01110100 01101000 01100001 01110100 00100000 01111001
01101111 01110101 00100000 01100100 01101001 01100100 01101110 00100111 01110100 00100000
01110101 01110011 01100101 00100000 01010111 01001110 01010011 00100000 01100101 01100001
01110010 01101100 01101001 01100101 01110010 00101110

Message

From: Jose Arteaga [j.arteaga@netzero.net]
Sent: 9/25/2020 10:29:12 AM
To: Alex Azar [alex.azar@hhs.gov]; Wheeler, Andrew [wheeler.andrew@epa.gov]; Ben Carson [ben.carson@hud.gov]; Chad Wolf [dhsexecsec@hq.dhs.gov]; Dan Brouillette [dan.brouillette@energy.gov]; David Bernhardt [david.berhardt@ios.doi.gov]; Elaine Chao [elaine.chao@dot.gov]; Elisabeth "Betsy" Prince DeVos [betsy.devos@ed.gov]; Eugene Scalia [executivesecretariat@dol.gov]; Federal Whistleblower ['DHSOIGHOTLINE@dhs.gov']; Gina Haspel [john.edwards@cia.gov]; John Ratcliffe [john.ratcliffe@dni.gov]; Jovita Carranza [jovita.carranza@sba.gov]; Kelly Craft [kelly.craft@un.org]; Mark Esper [mark.esper@dod.gov]; Mark Meadows [mark.meadows@whitehouse.gov]; Megan Smith [Ex. 6 Personal Privacy] Mike Pence [info@mike.pence.com]; Mike Pompeo [mike.pompeo@state.gov]; President Donald Trump [info@donaldtrump.com]; Robert E. Lighthizer [Ex. 6 Personal Privacy]; Robert Wilkie [robert.wilkie@va.gov]; Russ Vought [Ex. 6 Personal Privacy] Sonny Perdue [sonny.perdue@usda.gov]; Steve Mnuchin [steve.mnuchin@treasury.gov]; Wilbur Ross [wilbur.ross@commerce.gov]; William Barr [william.barr@justice.gov]
Subject: [SPAM-Sender] FW: Securing your website (Updated 7/24/2020) (1 of 14)

From: Jose Arteaga [mailto:j.arteaga@netzero.net]
Sent: Friday, September 25, 2020 3:29 AM
To: 'craig.mcpike@us.af.mil'; 'jerry.nix@cobb Galleria.com'; 'events@cobb Galleria.com'; 'services@cobb Galleria.com'; Andy Stein (astein@nnva.gov); Andy Stein (mgiardino@flyphf.com); Andy Stein (rford@flyphf.com); 'contactus@flyphf.com'; '311@nnva.gov'; 'william.caritj@atlanta.k12.ga.us'; 'suptoffice@atlanta.k12.ga.us'; 'ian.smith@atlanta.k12.ga.us'; 'billie.hart@nn.k12.va.us'; 'george.parker@nn.k12.va.us'; 'michelle.price@nn.k12.va.us'; 'patrick.finneran@nn.k12.va.us'; Michael Schubach (michael.schubach@trump.com); Michael Schubach (donald.trump@trump.com); Michael Schubach (allen.weisselberg@trump.com)
Subject: Securing your website (Updated 7/24/2020) (1 of 14)

Póngase en contacto con Servicio Commercial de EE.UU. <https://2016.export.gov/usoffices/index.asp> o *Web Network Shield* (WNS) 480-318-8020 o 418-271-6176 para una traducción en su idioma de elección.

01010111 01000101 01000010 00100000 01001110 01000101 01010100 01010111 01001111 01010010
01001011 00100000 01010011 01001000 01001001 01000101 01001100 01000100®

WNS®

Secure by Design

"Action without information is dangerous. Information without action is futile." ~ Arizona Tax Research Association

President Trump's schedule for September 25, 2020

(EDT)

- 2:00 PM Arrive at Dobbins Air Reserve Base – Atlanta, GA
- 2:20 PM Arrive at Cobb Galleria Centre – Atlanta, GA
- 2:40 PM Deliver remarks on Black Economic Empowerment: The Platinum Plan
- 3:55 PM Arrive at Dobbins Air Reserve Base – Atlanta, GA

- 5:35 PM Arrive at Joint Base Andrews – Washington, D.C.
- 6:10 PM Arrive at Trump International Hotel Washington, D.C.
- 6:45 PM Participate in a roundtable with supporters
- 7:55 PM Arrive at Joint Base Andrews – Washington, D.C.
- 8:50 PM Arrive at Newport News/Williamsburg International Airport – Newport News, VA
- 9:00 PM Deliver remarks at a Make America Great Again Event
- 10:30 PM The President has left Newport News, VA,

Data breaches continue to plague law organizations

(September 23, 2020) <http://www.bing.com/search?q=law%20data%20breach%20hack%20attack&qs=n&form=QBRE&sp=-1&pq=law%20data%20breach%20hack%20attack&sc=0-27&sk=&cvid=B71378DB1ACE466DB2B2FFDFF14AE9C9>

Data breaches continue to plague government organizations¹

Data breaches continue to plague education institutions²

Data breaches continue to plague distance learning

(August 22, 2020) <http://www.bing.com/search?q=distance+learning+data+breach+hack+attack&src=IE-SearchBox&FORM=IENTTR&conversationid=>

“We need very sharp people” ~ President Trump

WNS (Web Network Shield) has successfully demonstrated the effectiveness of its cyber-security product WNS to prevent all forms of URA (unauthorized remote access) to the New York Times, Wall Street Journal, Walmart, AT&T, Arizona Department of Water Resources, the U.S. Department of Defense, the U.S. House of Representatives, the U.S. Senate, The White House, the cities of Dallas, Phoenix, Tucson, Yuma, San Diego, Los Angeles, San Francisco, Sacramento, Washington D.C., New York City, the Trump Organization, the Catholic Church, Ohio and San Diego State University.

On September 12, 2020, while preparing a presentation for the city of Reno, NV, I needed to visit the city of Reno’s website <https://www.reno.gov/>. Unfortunately, there was a phishing malware program located within the city of Reno’s website. Fortunately, WNS was able to prevent URA (unauthorized remote access) as a result of that malware program.

“Show, don’t tell” ~ Storytellers

WNS wants to help protect your children, workers, and businesses from all forms of URA (unauthorized remote access). WNS will provide your organizations a free sample of part of our secure WNS web browser. If successful, the free demonstration will secure your websites only, not your IoT devices, from all forms of URA (unauthorized remote access).

Currently, WNS (Web Network Shield) has added your websites <https://www.dobbins.afrc.af.mil/>, <https://cobbgalleria.com/>, <https://www.trumphotels.com/washington-dc/luxury-washington-dc-hotels>, <https://flyphf.com/>, <https://www.atlantapublicschools.us/>, and <http://sbo.nn.k12.va.us/> to our favorite websites

list. This may improve the cyber-security of your websites. Today, September 25, 2020, at approximately 2:00 PM (EDT), WNS will remove <https://www.dobbins.afrc.af.mil/>, <https://cobb Galleria.com/>, <https://www.trumphotels.com/washington-dc/luxury-washington-dc-hotels>, <https://flyphf.com/>, <https://www.atlantapublicschools.us/>, and <http://sbo.nn.k12.va.us/> from our favorite websites list. This may affect the cyber-security of your websites.

“An ounce of prevention is worth a pound of cure response” ~ Benjamin Franklin (sort of)

WNS provides the following protection benefits:

- There is no need to obfuscate your email address because WNS protects your email address from phishing scams by immediately detecting and preventing all forms of URA (unauthorized remote access);
- There is no need to repeatedly change your username, password, or email address because WNS protects your email address by immediately detecting and preventing all forms of URA;
- WNS eliminates the need to update your security software (i.e. download malware and spyware URLs on your hard drive) because WNS debugs all all forms of URA. Downloading more than 350,000 malware strains daily will “crash” your device’s hard drive and render your device unusable;
- Protects your information against all forms of URA even if the attacker has your user name, password, and IP address.
- Provides a browser speed not throttled by spyware and/or extensions used to track user activity;
- Pass a penetration test from all forms of URA;
- Immediately detect and prevent all forms of URA;
- Secure a data transmission up to 200 feet.

“The cyber-attacks will continue until cyber-security improves” ~ a Hacker

It has been said it will require at least 12-18 months for an effective COVID-19 vaccine to be developed and distributed. The same can be said for the secure WNS web browser.

Cyber-crime in the U.S. has been declared a national emergency eight (8) times. Since 2017, lack of cyber-security has cost tax payers \$27 billion to \$56 billion per day.³

If President Trump doesn’t immediately begin the process of preparation, production and distribution of the secure WNS web browser, the U.S. may not be cyber-secure until 2022.

If you believe securing the your website by preventing all forms of URA (unauthorized remote access) is important, contact your Representative to prevent all forms of URA ASAP.

The WNS web browser is free to download.⁴ Contact your Representative <https://www.house.gov/representatives/find-your-representative>, Senator https://www.senate.gov/general/contact_information/senators_cfm.cfm, U. S. Commercial

Service <https://2016.export.gov/usoffices/index.asp> or Web Network Shield 480-318-8020 to protect your devices and information.

Web Network Shield mission statement:

Web Network Shield (WNS) seeks to become customer-focused, focusing our strategies and budgets on the technologies, systems and processes that win, serve and retain customers by immediately detecting and preventing URA from unregistered URLs, brute force programs, and mimicked IP addresses.

¹ The U.S. Outsources Cybersecurity & Defense To Contractors That Keep Getting Hacked

(May 3, 2013) <https://thinkprogress.org/the-u-s-outsources-cybersecurity-defense-to-contractors-that-keep-getting-hacked-abcb8b5a0c0a/>

Since 2005 over 9,000 data breaches have affected over 11.58 million records

(March 27, 2019) <https://www.privacyrights.org/data-breaches>

At least 693 breaches of government organizations have affected over 33.3 million records

(May 9, 2018)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=federal&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=federal&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=federal&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=state&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=state&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=state&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=county&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=county&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=county&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=city&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=city&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=city&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[my vocabulary 11 tid%5B%5D=273&taxonomy vocabulary 11 tid%5B%5D=272&taxonomy vocabulary 11 tid%5B%5D=271&=Search+Data+Breach](#)

² Education sector not taking \$7,370,000/year cyber threat cost seriously

(September 18, 2019) <https://pressreleases.responsesource.com/news/98403/education-sector-not-taking-7-370-000-year-cyber-threat-cost-seriously/>

Universities fail to learn the importance of cybersecurity, suffering over five devastating cyber attacks a semester.

... the education sector is one of the most heavily targeted industries by cyberattacks in its 2019 Global DNS Threat Report.

Over 500 US schools were hit by ransomware in 2019

Fifteen US school districts, accounting for 100 schools, were hit in the past two weeks alone.

(October 1, 2019) <https://www.zdnet.com/article/over-500-us-schools-were-hit-by-ransomware-in-2019/>

... found and tracked ransomware infections at 54 educational organizations like school districts and colleges, accounting for disruptions at over 500 schools.

To make matters worse, the attacks seem to have picked up in the last two weeks, with 15 school districts (accounting for over 100 K-12 schools) getting hit at the worst time possible -- in the first weeks of the new school year.

Overall, Connecticut saw ransomware infections hit seven school districts throughout 2019, making them the state whose educational institutions were compromised the most by ransomware attacks this year.

... based on currently available information we know that Crowder College of Neosho, Missouri, reported receiving the highest ransom demand among all school districts, with hackers requesting a whopping \$1.6 million to provide the district with means to decrypt its systems.

Last week, the US Senate passed a bill named the DHS Cyber Hunt and Incident Response Teams Act, which would create incident response teams to help private and public entities defend against cyber-attacks, such as ransomware attacks. The bill previously passed the House floor and is expected to be signed into law by the President in the coming months.

Over 1160 breaches of education organizations have affected over 43.6 million records¹

(May 10, 2018)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=school&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach)

[breaches?title=school&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach](#)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=education&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach)

[breaches?title=education&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach](#)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=university&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach)

[breaches?title=university&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach](#)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=college&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach)

[breaches?title=college&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach](#)

y vocabulary 11 tid%5B%5D=2257&taxonomy vocabulary 11 tid%5B%5D=2122&taxonomy vocabulary 11 tid%5B%5D=1473&taxonomy vocabulary 11 tid%5B%5D=1153&taxonomy vocabulary 11 tid%5B%5D=513&taxonomy vocabulary 11 tid%5B%5D=306&taxonomy vocabulary 11 tid%5B%5D=276&taxonomy vocabulary 11 tid%5B%5D=275&taxonomy vocabulary 11 tid%5B%5D=274&taxonomy vocabulary 11 tid%5B%5D=273&taxonomy vocabulary 11 tid%5B%5D=272&taxonomy vocabulary 11 tid%5B%5D=271&=Search+Data+Breaches

BACK TO SCHOOL

(December 13, 2018) <https://www.politico.com/newsletters/morning-cybersecurity>

The education sector comes in dead last when it comes to cybersecurity in 17 U.S. industries examined...

Identity theft isn't just an adult problem. Kids are victims, too

(April 28, 2018) <https://www.cnn.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html>

Child ID theft risks

Minors face some of the same risks as adults do, with their information being compromised in data breaches.

While adults make prime targets for their account balances, the "blank slate" a child provides can enable a criminal to do more damage by opening new lines of credit before someone catches on.

Protecting your kids

... experts say untangling identity theft and fraud committed against a minor is just as complicated as when an adult is the victim.

³ Cybercrime has cost more than \$10 trillion...

(October 27, 2017) <http://www.winknews.com/2017/10/27/cybercrime-has-cost-more-than-10-trillion-how-you-can-protect-yourself/>

Over \$27 billion per day!

Cost of cybercrime likely to hit \$21 trillion by 2021

(October 15, 2019) <https://www.ghanaweb.com/GhanaHomePage/business/Cost-of-cybercrime-likely-to-hit-21-trillion-by-2021-Ursula-789080>

Over \$56 billion per day!

Top 10 Most Expensive Disasters in U.S. History

(December 13, 2013) <https://www.trustedchoice.com/insurance-articles/weather-nature/most-expensive-disasters/>

1. Hurricane Katrina

•Cost: \$149 Billion

•Fatalities: 1,836

Why Cybersecurity Should Be A No. 1 Business Priority For 2017

(March 20, 2017) <https://www.forbes.com/sites/eycybersecurity/2017/03/20/why-cybersecurity-should-be-a-no-1-business-priority-for-2017/#371701681719>

Despite the evidence, most companies greatly understate the risk of a cyber incident...

This complacency makes little sense given the sharp uptick in hacking methods and sophistication. The average annual cost of cyberattacks to companies worldwide is pegged at more than \$9.5 million ...

Report: Average data breach costs public companies \$116m

(June 9, 2020) <https://www.complianceweek.com/cyber-security/report-average-data-breach-costs-public-companies-116m/29037.article>

... the average cost of a cyber-breach to a publicly traded company was \$116 million.

... the most common methods hackers successfully used to obtain company data from 2011 to 2019 was malware (34 percent)...

Why the 1# Vulnerability for Cyber Attacks Will Be Apathy

(March 17, 2015) <http://www.circleid.com/posts/20150317-why-the-1-vulnerability-for-cyber-attacks-will-be-apathy/>

How much do hackers love small companies? Some statistics:

•The U.S. Department of Homeland Security reports that 31 percent of all cyberattacks on business were aimed at companies with fewer than 250 employees.

•Symnatec Security Response discovered in 2012 that more than half of all targeted attacks focused on those businesses with fewer than 2,500 employees.

•Verizon's 2013 Data Breach Investigations Report said that mid-sized and small businesses experienced more data breaches than did larger firms.

Perhaps most frightening is the National Cyber Security Alliance's finding in 2012 that about 60 percent of all small companies go out of business within six months of a data breach!

We have some catching up to do on cyber-security

(February 20, 2015) <http://www.marketplace.org/topics/tech/big-book/we-have-some-catching-do-cyber-security>

Interviewed By Kai Ryssdal, Produced by Tommy Andres

•The Poneman Institute estimates it costs a company \$188 for every customer record stolen, from stopping the leak, bringing in outside consultants, replacing credit cards, lawsuits, etc. About 90 percent of small businesses that have customer information stolen go out of business within three years of an attack.

“One of the clear problems that we identified in the work of the commission was the fact that cyber responsibilities and accountability is scattered all over the federal government and there is no oversight and no consistent accountability...”

⁴ Lifeline Program for Low-Income Consumers

(April 27, 2020) <https://www.fcc.gov/general/lifeline-program-low-income-consumers>

Since 1985, the Lifeline program has provided a discount on phone service for qualifying low-income consumers to ensure that all Americans have the opportunities and security that phone service brings, including being able to connect to jobs, family and emergency services. Lifeline is part of the Universal Service Fund. The Lifeline program is available to eligible low-income consumers in every state, territory, commonwealth, and on Tribal lands.

The Federal government will subsidize the cost of WNS in a program similar to subsidized cell phones, HUD Section 8 rent, and medical insurance.

This electronic message, including any attachments, is for the use of the intended recipient(s) only. If you have received this message in error, please notify the sender immediately and then delete it. Measures have been taken to eliminate the risk of transmitting software viruses but please be advised to conduct your own virus checks on any attachment to this message. If you are the intended recipient and you do not wish to receive similar electronic messages from us in the future then please respond to the sender to this effect.

01010100 01101000 01100101 00100000 01101111 01101110 01101100 01111001 00100000 01110100
01101000 01101001 01101110 01100111 00100000 01111001 01101111 01110101 00100000 01110111
01101001 01101100 01101100 00100000 01110010 01100101 01100111 01110010 01100101 01110100
00100000 01101001 01110011 00100000 01110100 01101000 01100001 01110100 00100000 01111001

01101111 01110101 00100000 01100100 01101001 01100100 01101110 00100111 01110100 00100000
01110101 01110011 01100101 00100000 01010111 01001110 01010011 00100000 01100101 01100001
01110010 01101100 01101001 01100101 01110010 00101110

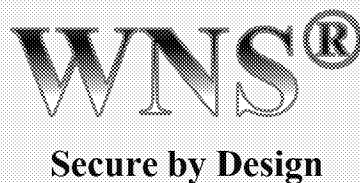
Message

From: Jose Arteaga [j.arteaga@netzero.net]
Sent: 9/13/2020 12:14:40 PM
To: Alex Azar [alex.azar@hhs.gov]; Wheeler, Andrew [wheeler.andrew@epa.gov]; Ben Carson [ben.carson@hud.gov]; Chad Wolf [dhsexecsec@hq.dhs.gov]; Dan Brouillette [dan.brouillette@energy.gov]; David Bernhardt [david.berhardt@ios.doi.gov]; Elaine Chao [elaine.chao@dot.gov]; Elisabeth "Betsy" Prince DeVos [betsy.devos@ed.gov]; Eugene Scalia [executivesecretariat@dol.gov]; Federal Whistleblower [DHSOIGHOTLINE@dhs.gov]; Gina Haspel [john.edwards@cia.gov]; John Ratcliffe [john.ratcliffe@dni.gov]; Jovita Carranza [jovita.carranza@sba.gov]; Kelly Craft [kelly.craft@un.org]; Mark Esper [mark.esper@dod.gov]; Mark Meadows [mark.meadows@whitehouse.gov]; Megan Smith [Ex. 6 Personal Privacy]; Mike Pence [info@mike.pence.com]; Mike Pompeo [mike.pompeo@state.gov]; President Donald Trump [info@donaldtrump.com]; Robert E. Lighthizer [Ex. 6 Personal Privacy]; Robert Wilkie [robert.wilkie@va.gov]; Russ Vought [Ex. 6 Personal Privacy]; Sonny Perdue [sonny.perdue@usda.gov]; Steve Mnuchin [steve.mnuchin@treasury.gov]; Wilbur Ross [wilbur.ross@commerce.gov]; William Barr [william.barr@justice.gov]
Subject: [SPAM-Sender] FW: Securing your website (Updated 7/24/2020) (1 of 15)

From: Jose Arteaga [mailto:j.arteaga@netzero.net]
Sent: Sunday, September 13, 2020 5:14 AM
To: 'phil.ruffin@ruffincompanies.com'; 'TI-Casino-Marketing@treasureisland.com'; 'TI-General@treasureisland.com'; 'jeanette.nunez@latinos.donaldjtrump.com'; 'maggie.hernandez@latinos.donaldjtrump.com'; 'sergio.arellano@latinos.donaldjtrump.com'; 'jeffjsc@xmfg.com'; 'matthew.elvin@xmfg.com'; 'amelia@xmfg.com'; 'info@xmfg.com'; 'Alyssa.Rodriguez@cityofhenderson.com'; 'Debra.March@cityofhenderson.com'; 'Ryan.Turner@cityofhenderson.com'; Michael Schubach (michael.schubach@trump.com); Michael Schubach (donald.trump@trump.com); Michael Schubach (allen.weisselberg@trump.com)
Cc: Alan Cunningham (alan.cunningham@admin.nv.gov); Alan Cunningham (governor@govmail.state.nv.us); Alan Cunningham (sosexec@sos.nv.gov)
Subject: Securing your website (Updated 7/24/2020) (1 of 15)

Póngase en contacto con Servicio Commercial de EE.UU. <https://2016.export.gov/usoffices/index.asp> o *Web Network Shield* (WNS) 480-318-8020 o 418-271-6176 para una traducción en su idioma de elección.

01010111 01000101 01000010 00100000 01001110 01000101 01010100 01010111 01001111 01010010
01001011 00100000 01010011 01001000 01001001 01000101 01001100 01000100®



“Action without information is dangerous. Information without action is futile.” ~ Arizona Tax Research Association

President Trump's schedule for September 13, 2020

9:55 AM Arrive at Treasure Island – TI Hotel & Casino

10:00 AM Participate in a Latinos for Trump Coalition Roundtable

11:15 AM Participate in a roundtable with supporters – Las Vegas, NV

12:10 PM Arrive at Trump International Hotel Las Vegas
5:40 PM Arrive at Xtreme Manufacturing – Henderson, NV
6:15 PM Participate in a roundtable with supporters – Henderson, NV
7:00 PM Deliver remarks Live from Nevada
8:15 PM The President has left Henderson, NV

Data breaches continue to plague airports

(September 10, 2020) <http://www.bing.com/search?q=airport+data+breach+hack+attack&src=IE-SearchBox&FORM=IENTTR&conversationid=>

Data breaches continue to plague government organizations¹

Data breaches continue to plague education institutions²

Data breaches continue to plague distance learning

(August 22, 2020) <http://www.bing.com/search?q=distance+learning+data+breach+hack+attack&src=IE-SearchBox&FORM=IENTTR&conversationid=>

WNS (Web Network Shield) has successfully demonstrated the effectiveness of its cyber-security product WNS to prevent all forms of URA (unauthorized remote access) to the New York Times, Wall Street Journal, Walmart, AT&T, Arizona Department of Water Resources, the U.S. Department of Defense, the U.S. House of Representatives, the U.S. Senate, The White House, the cities of Dallas, Phoenix, Tucson, Yuma, San Diego, Los Angeles, San Francisco, Sacramento, Washington D.C., New York City, the Trump Organization, the Catholic Church, and San Diego State University.

On September 12, 2020, while preparing a presentation for Reno, NV, I needed to visit Reno, NV's website <https://www.reno.gov/>. Unfortunately, there was a phishing malware located at Reno, NV's website. Fortunately, WNS was able to prevent URA (unauthorized remote access) as a result of that malware.

"Show, don't tell" ~ Storytellers

WNS wants to help protect your children, workers, and businesses from all forms of URA (unauthorized remote access). WNS will provide your organizations a free sample of part of our secure WNS web browser. If successful, the free demonstration will secure your websites only, not your IoT devices, from all forms of URA (unauthorized remote access).

Currently, WNS (Web Network Shield) has added your websites https://treasureisland.com/?gclid=CNKE-dqC5usCFYYmfwodepQE_g&gclid=ds, <https://latinos.donaldjtrump.com/>, https://www.trumphotels.com/las-vegas?msclkid=d03d766fa19f153145742931aa22db98&utm_source=bing&utm_medium=cpc&utm_campaign=MI%20Trump%20Hotels%20Las%20Vegas%20Brand&utm_term=trump%20international%20hotel%20las%20vegas&utm_content=Brand%20Las%20Vegas%20Hotel, <https://www.xmfg.com/>, and <https://www.cityofhenderson.com/> to our favorite websites list. This may improve the cyber-security of your websites. Today, September 13, 2020, at

approximately 2:30 PM (MDT), WNS will remove https://treasureisland.com/?gclid=CNKE-dqC5usCFYYmfwodepQE_g&gclid=ds, <https://latinos.donaldjtrump.com/>, https://www.trumphotels.com/las-vegas?msclkid=d03d766fa19f153145742931aa22db98&utm_source=bing&utm_medium=cpc&utm_campaign=MI%20Trump%20Hotels%20Las%20Vegas%20Brand&utm_term=trump%20international%20hotel%20las%20vegas&utm_content=Brand%20Las%20Vegas%20Hotel, <https://www.xmfg.com/>, and <https://www.cityofhenderson.com/> from our favorite websites list. This may affect the cyber-security of your websites.

“An ounce of prevention is worth a pound of cure response” ~ Benjamin Franklin (sort of)

WNS provides the following protection benefits:

- There is no need to obfuscate your email address because WNS protects your email address from phishing scams by immediately detecting and preventing all forms of URA (unauthorized remote access);
- There is no need to repeatedly change your username, password, or email address because WNS protects your email address by immediately detecting and preventing all forms of URA;
- WNS eliminates the need to update your security software (i.e. download malware and spyware URLs on your hard drive) because WNS debugs all all forms of URA. Downloading more than 350,000 malware strains daily will “crash” your device’s hard drive and render your device unusable;
- Protects your information against all forms of URA even if the attacker has your user name, password, and IP address.
- Provides a browser speed not throttled by spyware and/or extensions used to track user activity;
- Pass a penetration test from all forms of URA;
- Immediately detect and prevent all forms of URA;
- Secure a data transmission up to 200 feet.

“The cyber-attacks will continue until cyber-security improves” ~ a Hacker

It has been said it will require at least 12-18 months for an effective COVID-19 vaccine to be developed and distributed. The same can be said for the secure WNS web browser.

Cyber-crime in the U.S. has been declared a national emergency eight (8) times. Since 2017, lack of cyber-security has cost tax payers \$27 billion to \$56 billion per day.³

If President Trump doesn’t immediately begin the process of preparation, production and distribution of the secure WNS web browser, the U.S. may not be cyber-secure until 2022.

If you believe securing the your website by preventing all forms of URA (unauthorized remote access) is important, contact your Representative to prevent all forms of URA ASAP.

The WNS web browser is free to download.⁴ Contact your Representative <https://www.house.gov/representatives/find-your-representative>, Senator https://www.senate.gov/general/contact_information/senators_cfm.cfm, U. S. Commercial Service <https://2016.export.gov/usoffices/index.asp> or Web Network Shield 480-318-8020 to protect your devices and information.

Web Network Shield mission statement:

Web Network Shield (WNS) seeks to become customer-focused, focusing our strategies and budgets on the technologies, systems and processes that win, serve and retain customers by immediately detecting and preventing URA from unregistered URLs, brute force programs, and mimicked IP addresses.

¹ The U.S. Outsources Cybersecurity & Defense To Contractors That Keep Getting Hacked

(May 3, 2013) <https://thinkprogress.org/the-u-s-outsources-cybersecurity-defense-to-contractors-that-keep-getting-hacked-abcb8b5a0c0a/>

Since 2005 over 9,000 data breaches have affected over 11.58 million records

(March 27, 2019) <https://www.privacyrights.org/data-breaches>

At least 693 breaches of government organizations have affected over 33.3 million records

(May 9, 2018)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=federal&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=federal&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=federal&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=state&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=state&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=state&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=county&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=county&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=county&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=city&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[breaches?title=city&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches](https://www.privacyrights.org/data-breaches?title=city&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches)

[B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach](#)

2 Education sector not taking \$7,370,000/year cyber threat cost seriously

(September 18, 2019) <https://pressreleases.responsesource.com/news/98403/education-sector-not-taking-7-370-000-year-cyber-threat-cost-seriously/>

Universities fail to learn the importance of cybersecurity, suffering over five devastating cyber attacks a semester.

... the education sector is one of the most heavily targeted industries by cyberattacks in its 2019 Global DNS Threat Report.

Over 500 US schools were hit by ransomware in 2019

Fifteen US school districts, accounting for 100 schools, were hit in the past two weeks alone.

(October 1, 2019) <https://www.zdnet.com/article/over-500-us-schools-were-hit-by-ransomware-in-2019/>

... found and tracked ransomware infections at 54 educational organizations like school districts and colleges, accounting for disruptions at over 500 schools.

To make matters worse, the attacks seem to have picked up in the last two weeks, with 15 school districts (accounting for over 100 K-12 schools) getting hit at the worst time possible -- in the first weeks of the new school year.

Overall, Connecticut saw ransomware infections hit seven school districts throughout 2019, making them the state whose educational institutions were compromised the most by ransomware attacks this year.

... based on currently available information we know that Crowder College of Neosho, Missouri, reported receiving the highest ransom demand among all school districts, with hackers requesting a whopping \$1.6 million to provide the district with means to decrypt its systems.

Last week, the US Senate passed a bill named the DHS Cyber Hunt and Incident Response Teams Act, which would create incident response teams to help private and public entities defend against cyber-attacks, such as ransomware attacks. The bill previously passed the House floor and is expected to be signed into law by the President in the coming months.

Over 1160 breaches of education organizations have affected over 43.6 million records¹

(May 10, 2018)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=school&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach)

[breaches?title=school&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach](#)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=education&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach)

[breaches?title=education&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach](#)

[https://www.privacyrights.org/data-](https://www.privacyrights.org/data-breaches?title=university&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach)

[breaches?title=university&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breach](#)

https://www.privacyrights.org/data-breaches?title=college&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257&taxonomy_vocabulary_11_tid%5B%5D=2122&taxonomy_vocabulary_11_tid%5B%5D=1473&taxonomy_vocabulary_11_tid%5B%5D=1153&taxonomy_vocabulary_11_tid%5B%5D=513&taxonomy_vocabulary_11_tid%5B%5D=306&taxonomy_vocabulary_11_tid%5B%5D=276&taxonomy_vocabulary_11_tid%5B%5D=275&taxonomy_vocabulary_11_tid%5B%5D=274&taxonomy_vocabulary_11_tid%5B%5D=273&taxonomy_vocabulary_11_tid%5B%5D=272&taxonomy_vocabulary_11_tid%5B%5D=271&=Search+Data+Breaches

BACK TO SCHOOL

(December 13, 2018) <https://www.politico.com/newsletters/morning-cybersecurity>

The education sector comes in dead last when it comes to cybersecurity in 17 U.S. industries examined...

Identity theft isn't just an adult problem. Kids are victims, too

(April 28, 2018) <https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html>

Child ID theft risks

Minors face some of the same risks as adults do, with their information being compromised in data breaches.

While adults make prime targets for their account balances, the "blank slate" a child provides can enable a criminal to do more damage by opening new lines of credit before someone catches on.

Protecting your kids

... experts say untangling identity theft and fraud committed against a minor is just as complicated as when an adult is the victim.

³ Cybercrime has cost more than \$10 trillion...

(October 27, 2017) <http://www.winknews.com/2017/10/27/cybercrime-has-cost-more-than-10-trillion-how-you-can-protect-yourself/>

Over \$27 billion per day!

Cost of cybercrime likely to hit \$21 trillion by 2021

(October 15, 2019) <https://www.ghanaweb.com/GhanaHomePage/business/Cost-of-cybercrime-likely-to-hit-21-trillion-by-2021-Ursula-789080>

Over \$56 billion per day!

Top 10 Most Expensive Disasters in U.S. History

(December 13, 2013) <https://www.trustedchoice.com/insurance-articles/weather-nature/most-expensive-disasters/>

1. Hurricane Katrina

•Cost: \$149 Billion

•Fatalities: 1,836

Why Cybersecurity Should Be A No. 1 Business Priority For 2017

(March 20, 2017) <https://www.forbes.com/sites/eycybersecurity/2017/03/20/why-cybersecurity-should-be-a-no-1-business-priority-for-2017/#371701681719>

Despite the evidence, most companies greatly understate the risk of a cyber incident...

This complacency makes little sense given the sharp uptick in hacking methods and sophistication. The average annual cost of cyberattacks to companies worldwide is pegged at more than \$9.5 million...

Report: Average data breach costs public companies \$116m

(June 9, 2020) <https://www.complianceweek.com/cyber-security/report-average-data-breach-costs-public-companies-116m/29037.article>

... the average cost of a cyber-breach to a publicly traded company was \$116 million.

... the most common methods hackers successfully used to obtain company data from 2011 to 2019 was malware (34 percent)...

Why the 1# Vulnerability for Cyber Attacks Will Be Apathy

(March 17, 2015) http://www.circleid.com/posts/20150317_why_the_1_vulnerability_for_cyber_attacks_will_be_apathy/

How much do hackers love small companies? Some statistics:

•The U.S. Department of Homeland Security reports that 31 percent of all cyberattacks on business were aimed at companies with fewer than 250 employees.

•Symnatec Security Response discovered in 2012 that more than half of all targeted attacks focused on those businesses with fewer than 2,500 employees.

•Verizon's 2013 Data Breach Investigations Report said that mid-sized and small businesses experienced more data breaches than did larger firms.

Perhaps most frightening is the National Cyber Security Alliance's finding in 2012 that about 60 percent of all small companies go out of business within six months of a data breach!

We have some catching up to do on cyber-security

(February 20, 2015) <http://www.marketplace.org/topics/tech/big-book/we-have-some-catching-do-cyber-security>

Interviewed By Kai Ryssdal, Produced by Tommy Andres

•The Poneman Institute estimates it costs a company \$188 for every customer record stolen, from stopping the leak, bringing in outside consultants, replacing credit cards, lawsuits, etc. About 90 percent of small businesses that have customer information stolen go out of business within three years of an attack.

“One of the clear problems that we identified in the work of the commission was the fact that cyber responsibilities and accountability is scattered all over the federal government and there is no oversight and no consistent accountability...”

4 Lifeline Program for Low-Income Consumers

(April 27, 2020) <https://www.fcc.gov/general/lifeline-program-low-income-consumers>

Since 1985, the Lifeline program has provided a discount on phone service for qualifying low-income consumers to ensure that all Americans have the opportunities and security that phone service brings, including being able to connect to jobs, family and emergency services. Lifeline is part of the Universal Service Fund. The Lifeline program is available to eligible low-income consumers in every state, territory, commonwealth, and on Tribal lands.

The Federal government will subsidize the cost of WNS in a program similar to subsidized cell phones, HUD Section 8 rent, and medical insurance.

This electronic message, including any attachments, is for the use of the intended recipient(s) only. If you have received this message in error, please notify the sender immediately and then delete it. Measures have been taken to eliminate the risk of transmitting software viruses but please be advised to conduct your own virus checks on any attachment to this message. If you are the intended recipient and you do not wish to receive similar electronic messages from us in the future then please respond to the sender to this effect.

01010100 01101000 01100101 00100000 01101111 01101110 01101100 01111001 00100000 01110100
01101000 01101001 01101110 01100111 00100000 01111001 01101111 01110101 00100000 01110111
01101001 01101100 01101100 00100000 01110010 01100101 01100111 01110010 01100101 01110100
00100000 01101001 01110011 00100000 01110100 01101000 01100001 01110100 00100000 01111001
01101111 01110101 00100000 01100100 01101001 01100100 01101110 00100111 01110100 00100000
01110101 01110011 01100101 00100000 01010111 01001110 01010011 00100000 01100101 01100001
01110010 01101100 01101001 01100101 01110010 00101110